Radio Frequency Identification (RFID) Tags

&

Their Implication to Container Security

Joseph Benin

13 April 2004

INTA 8803N
International Security Seminar
Sam Nunn Security Program

Report Documentation Page	*Form Approved OMB No. 0704-0188*

1. REPORT DATE **13 APR 2004**	2. REPORT TYPE	3. DATES COVERED **00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE **Radio Frequency Identification (RFID) Tags & Their Implication to Container Security**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Coast Guard Academy ,31 Mohegan Avenue ,New London ,CT,06320-8103**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**28**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Introduction

From a security standpoint, the state of container security throughout this nation and the world's ports is frightening. The situation has been well documented and is receiving support throughout Congress to increase funding for related research projects. Regrettably, due to the physical, political, and economic complexity of the system, research is virtually all that has been done to physically secure individual containers. While Customs and Border Patrol have launched a series of programs to increase the "layers of defense" at U.S. ports (e.x. C-TPAT and CSI), the actual projects of Operation Safe Commerce and their current status remain undisclosed, and our ports remain unprotected.

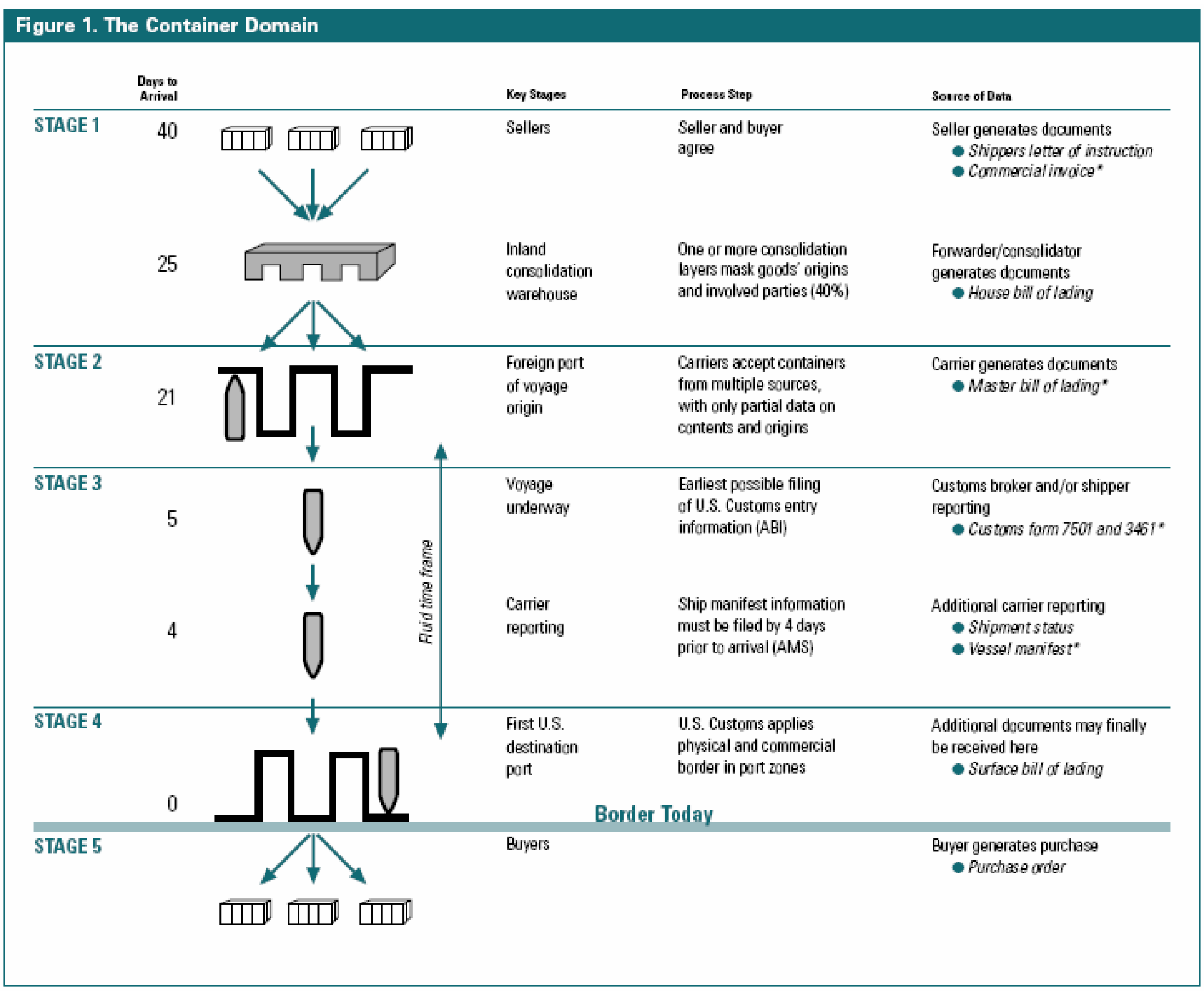

Figure 1 - Virtual Border Methodology [1]

Plan to Fully Secure Ocean-Going Containers

To date, at least two comprehensive, informed, and realistic plans to secure ocean-going trade have been published. In August of 2002, an article was published in Defense Horizons entitled "The Virtual Border: Countering Seaborne Container Terrorism." Their proposed plan to secure seaborne containers is presented in Figure 1. It outlines the paper trail required for international container shipments, a timetable for actions, and the various sensors available to detect nuclear, chemical, and explosive materials.

In January of 2003, the Center for International Security and Cooperation (CISAC) of the Institute for International Studies (IIS) at Stanford University released a study entitled "Container Security Report" [2]. This report outlined an even broader approach to securing sea trade lanes and categorizes the three major challenge areas as:

1. Technical – Equipment and System Design, and Research Management
2. Economic – Anticipating the Costs of Required Technical and Human Investments, and Determining Who will Bear those Costs
3. Institutional – Overcoming Domestic and International Impediments to Securing Cooperation from Various Market Participants, Interest Groups, and Nation-States

Their sample technical approach contained four "site-specific stages" of operation and one "continuous system-wide function" [2]. They are:

- Certification of the packing of individual containers
- Security procedures at the port of embarkation
- Continued monitoring during transit after containers have been loaded onto a ship
- Security procedures at the port of debarkation
- Continuous collection and fusion of data regarding the movement of individual shipments of goods in a computer system. The system should be designed to fail gracefully under physical or cyber attack on some of its components.

The CISAC study's conceptual cargo flowchart is shown in Figure 2.

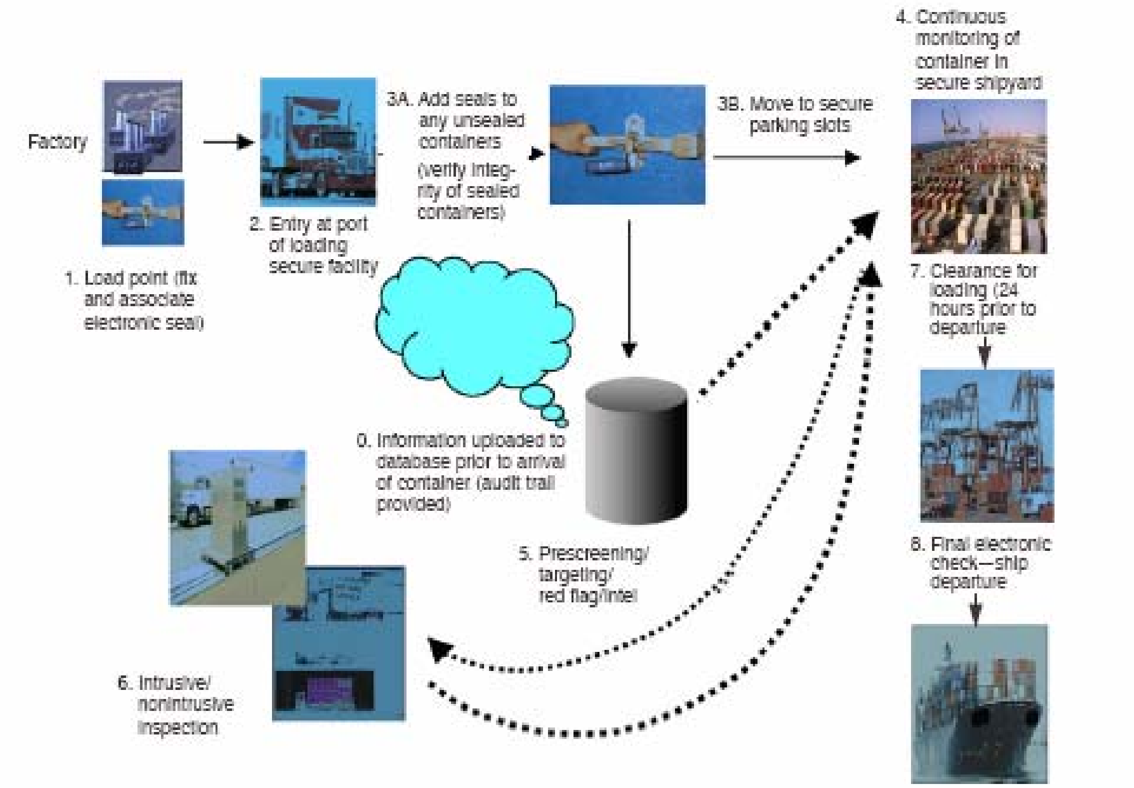

Figure 1. Cargo Flow and Monitoring at Ports of Embarkation

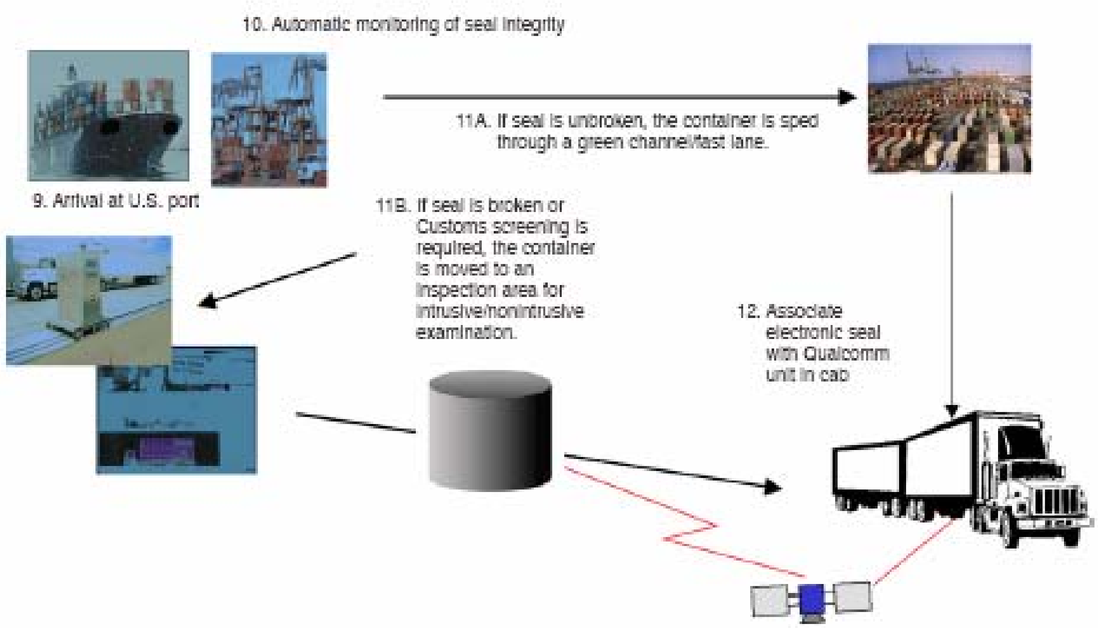

Figure 2 - Stanford Secure Flow Diagram [2]

Research Paper Scope

A complete analysis of the international sea-going container system is beyond the scope of this project. Instead, the goal of this project was to research two keynote technologies presently being tested for use in securing sea-borne container trade. During the project proposal phase, a thorough survey of scholarly journals and readily available reports on the Internet identified RFIDs and Electronic Seals (E-Seals) as being among the most promising proximate technologies for securing trade. RFIDs attempt to help solve the problem of knowing what is inside a container's opaque construction and densely packed contents, while E-Seals were to assist in verifying that the contents of a given container have not been tampered with. Additional research has found that the term "E-Seal" is used inconsistently. While some use it as defined in this project's proposal [3], almost all literature defines E-Seals as the *active* subset of RFIDs, which can be either active or passive (see discussion below).

This paper seeks to introduce the reader to the world of RFID, examine some of the technical aspects of the technologies encompassed, discuss two of the greatest technical hurdles to implementing this technology, look at current applications of RFID, and survey the future of this technology.

RFID History

The use of radio frequencies to transmit data from stored tags is not new. In fact, the RFID concept was first devised in the late 1940's to identify aircraft in radar [4]. While the technology slowly evolved over time and transitioned into the commercial market, it did not branch out of the aerospace industry until the mid 1980's when the Dutch government sought a method to uniquely identify 75 million "items" that were difficult to label using standard methods. It was noted that "identification would greatly improve efficiency of handling,

production and later processing” as well as help control black market imports from Germany [4]. As M.M. Ollivier states in “RFID – A Practical Solution for Problems You Didn’t Even Know You Had!”:

> “The items had flexible surfaces unsuitable for gluing, few structural regions for tag attachment, were often exposed to weather, routinely caked in dirt, and not easily constrained to a fixed location. The items were pigs, and the result was the electronic tag.”

This resulted in the robust, small, and sealed design of battery-less tags. This commercial application began a trend of use for RFIDs beyond aviation and has since sparked tremendous research and development into this technology with much promise for greater levels of efficiency and security than ever before.

Initially, RFIDs were read-only devices that came encoded at manufacturing. While this preserved the integrity of the data stored, it limited their usefulness and made them little more than expensive barcodes. In time, read/write tags were developed that allowed the end user to reprogram the tags over 10,000 times [4]. This expanded their use and resulted in greater production levels and subsequently reduced per-tag costs. However, this new strength of being re-writeable was also a weakness. Now identification numbers were no longer unique and integrity could no longer be assured. This first problem was solved with the introduction of multi-page tags. The first multi-page (M/P) tag contained seventeen “pages” of 64 bits, such that the first page was a unique, read-only (R/O) identification number, and the remaining sixteen pages were re-writeable with the option of the user making them R/O [4]. Today, RFIDs come in many different configurations, the details of which will be discussed next.

RFID Preliminaries

An array of technologies actually comprise what is colloquially referred to as “RFID.” A basic definition as to what qualifies as an RF Identification device is:

> "a base radio transmitter/receiver, or reader, which can interrogate, display, and sometimes rewrite, an electronic code held in a remote device, transponder, and thus identify any item with which the transponder is associated" [4].

This can be distilled to the basic purpose of RFID (also called Dedicated Short Range Communication (DSRC) within Electrical Engineering circles) as creating a "wireless link to uniquely identify objects or people" [5].

There are actually two separate but related technologies within the umbrella of RFID: Active and Passive. While normally discussed interchangeably, active and passive RFIDs "are fundamentally distinct technologies with substantially different capabilities" [6]. The primary distinguishing characteristic between active and passive RFIDs is their source of power. A passive RFID tag is not powered in and of itself; rather, it must be powered by an external source. For active RFID tags, power is internal to the tag itself. Table 1 highlights the differences between active and passive RFID tags.

	Active RFID	Passive RFID
Tag Power Source	Internal	External
Tag Battery	Yes	No
Availability of Tag Power	Continuous	Only within Field of Reader
Required Signal Strength from Reader to Tag	Low	High (Must Power the Tag)
Available Signal Strength from Tag to Reader	High	Low
Communication Range	Long (~100m)	Short (<3m)
Multi-Tag Collection	1000's of Tags over 7 Acres	Up to 300 tags within 3 meters
	20 Tags Moving at 100 mph	20 Tags Moving at 3 mph
Sensor Capability	Can Continuously Monitor and Record Sensor Input and Include Date/Time Stamp	Only Read/Transfer Sensor Values when Tag Powered by Reader; No Date/Time Stamp
Data Storage	Large (128kb Mag)	Small (128b Mag)

Source: Active and Passive RFID

Table 1 - Summary of Functional Capabilities of Active and Passive RFID Technologies

Passive RFID

Originally, passive tags were strictly limited to read-only capabilities. However more recently they have embodied very limited write functionality. The Figure 3 "shows a variety of Texas Instruments passive mid-frequency 13.56-MHz tags, with a 256-bit read/write memory

organized into eight 32-bit blocks" [7]. These blocks in turn can be made read-only by the user. The transmission rate with these RFID labels is 9 to 27 kilobits.

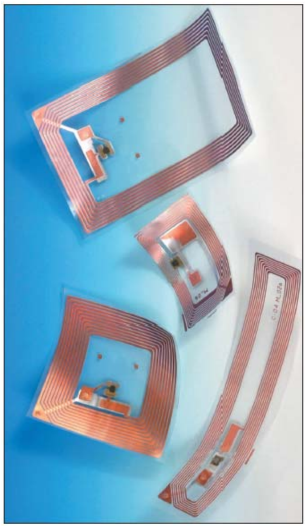

Figure 3 - Passive TI RFIDs

Active RFID (a.k.a. Electronic Seals)

Within the overall "layered defense" of container security, the fact remains that active RFID tags can interface with a myriad of sensors (including light, temperature, humidity, vibration, access, position, acceleration, gamma rays, chemical signatures, etc). This makes the gains from the use of active RFID exceptional.

Electronic Seals within this category normally include a physical sensor that detects a break in cable continuity, thus indicating that someone has broken the seal [3]. Additionally, light and heat sensors can be used to determine if someone has gained access from another portion of the container.

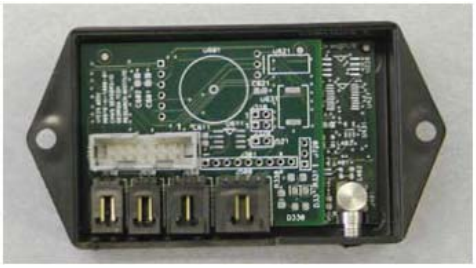

Figure 4 - Prototype GTRI Active RFID

An example of an active RFID tag is that being developed by the Georgia Tech Research Institute (GTRI) [19]. Their project, as explained to me by GTRI's Dr. Giselle Bennett, is part of the U.S. Navy's Logistics and Maintenance Applied Research Center (LandMARC) program. It is a real-time integrated sensor radio frequency identification system (ISFRID). Their active RFID prototype, see Figure 4, is presently deployed and tracking assets of high value. Its primary goals are to provide real-time data on an asset's readiness (condition), accuracy (true identification), and location ("total asset visibility"). Their pilot program includes not only the RFID, but also integrated sensors, the infrastructure necessary to read the RFIDs and store and

transmit their data, and also the software necessary to manage the related information. For additional information regarding this project, the interested reader is referred to http://landmarc.gtri.gatech.edu/.

Total Asset Visibility (TAV)

Initiated in 1995, the TAV was the brainchild of the Defense Logistics Agency (DLA) to provide real-time logistics information regarding system performance, automatically order replacement components for failing equipment, and provide real-time tracking of that equipment in route [8].

This program is significant because it is considered the first testing of RFID tags for global tracking. The first shipment was hazardous materials (HAZMAT) through the DOD supply chain [8]. A battery of tests involving environmental, ruggedness, technology and process validation, and a real world validation were planned. On June, 6, 2001, sources were sought for the RFID technology [8]. Two vendor groups were ultimately selected and the results of the tests are summarized in table 2.

Environmental	some degradation in read rates at low temps and with in-band RF interference
Ruggedness	No significant degradation after stack, vibration, and drop tests
Technology and Process Validation	Both tags could be read simultaneously, but performance varied by tag type, packaging material, and orientation
Real World	Damage to some tags, but no significant reduction in readability

Source: MICLOG RFID Tag Program Enables Total Asset Visibility

Table 2 - TAV Test Results

The TAV project demonstrated (and continues to demonstrate) the potential of RFID within the United States and paved the way for the expansion of this technology in the global supply chain. Three outcomes of the project were the identification of the need for standards, the improvement of multi-band antennas, and smaller power sources [8].

How RFIDs Work

The two components of an RFID system are the RFID and the Reader. These communicate via radio signals either uni-directionally or bi-directionally [5]. RFIDs can use single frequencies or dual frequencies for this communication. When a tag enters the range of a reader, its information is extracted and transmitted by the reader to any electronic device, such as a real-time display (ex. monitor or printer), a storage device, a network device for forwarding, or a programmable logic controller for action [5]. This process is pictured in the following figure below.

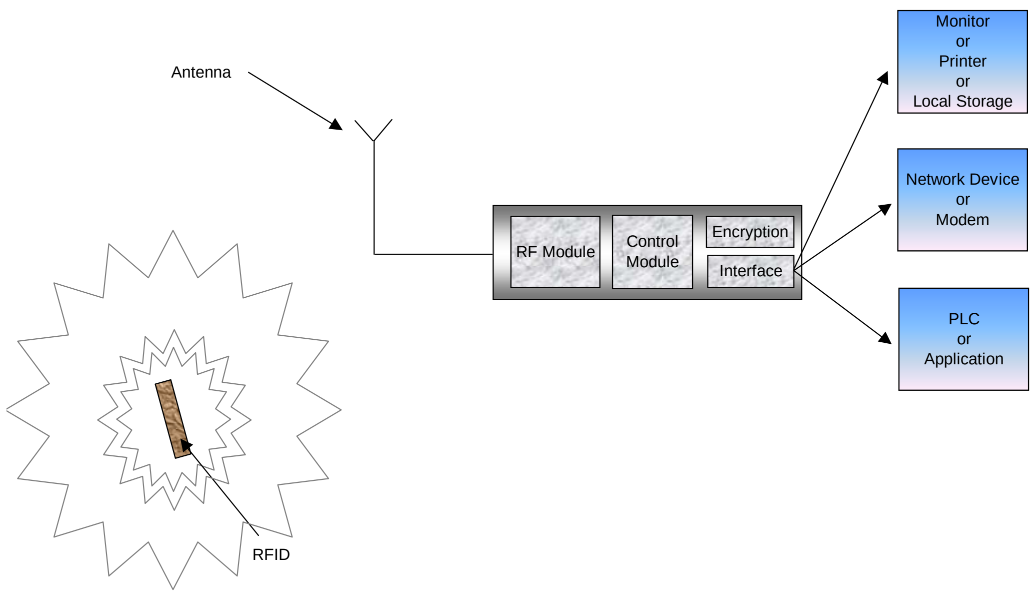

Figure 5 - RFID Process [5]

Key RFID Features [18]

In order to understand how RFID tags can be implemented for use in any given application, including container security, it is important to also know some of their key features. While at their most basic level RFIDs are glamorized barcodes, the fact is that they contain capabilities an order of magnitude greater than their black and white predecessors. In the end, RFID has the potential to revolutionize how processes are managed, businesses are operated, and even inspire new automated solutions [5].

Line of Sight

RFIDs do not require a clear line of sight between the tag and reader. They can be read, depending on signal strength and environmental conditions, through all manner of boundaries including plastic, water, and metals.

Robustness

The fact that RFIDs do not need to be in plain view allows them to be placed in hardened cases. This provides for greater robustness within the device as well as more ideal placements that are less likely to be scraped or subject to shock. This results in high reliability rates, even in the harshest of environments.

Read Characteristics

The time it takes to process labeled goods is drastically reduced since an RFID reader can scan multiple tags simultaneously and from greater distances,. This enables tracking of individual items; not just pallets or boxes. This eliminates manual data entry and the corresponding delays and errors introduced.

Physical Security

The enclosed cases of the seals make them more difficult to physically tamper. Furthermore, as they are not in view, they are less likely to be subjected to whimsical physical handling. Finally, most RFIDs have internal circuitry that will alert a reader of its poor health should it be opened or damaged.

Programmability

The ability of a user to store information on the tag itself allows for much greater depth of information flow and efficiency. Processes can be recorded or personnel can “sign” when they inspected the item. Above all, the tags can be reused many times over for economic savings.

Flexibility [5]

Another advantage of RFID is design flexibility. RFIDs can be manufactured in any number of shapes, sizes, forms, materials, and can even be integrated in a product itself, such as the fabric of a shirt.

Cost

The cost of RFID tags is as varied as the features they provide. In mass quantity, passive RFIDs with minimal data capacity can cost as little as five cents each. Active RFIDs with expansive capabilities and a sizeable amount of storage, small footprint, and prolonged battery life can cost over $500.00 each.

RFID Technical Considerations

Standards

The need for standardization (within the area of security in general and RFIDs in particular) is a two-sided issue. It is both a common criticism and compliment throughout industry, government, and academia. On one side, “standards provide a neutral ground where methodologies are established that advance the interests of manufacturers as well as consumers, while providing assurances of safety and reliability.” On the other side, those who desire greater openness argue that “standards can be inappropriately employed to favor some vendors’ products over others, make competition costly, and encourage mediocrity over innovation” resulting in weaker levels of security [9].

While there is no shortage of standardization bodies (ANSI, ISO, IEEE, NIST, and W3C to name a few), there has yet to be a definitive standard set for RFID protocol, frequency, hardware interface, or data format. This lack of an accepted global standard has been attributed as one of the greatest impediments to global RFID proliferation.

Specific areas in need of standards include communication systems protocols, unique identification code coordination and format, sensor communications, and synchronization and transport of precise time [8]. While it is true that work has been conducted in these areas, such as IPv6 for the first category and IEEE 1588 for the last, these have not been adapted for use with RFID or to form a comprehensive platform for use.

One standard that does exist, however, is “Identification Cards – Contactless Integrated Circuit(s) Cards – Vicinity Cards” that some view as the first step in standardizing RFIDs. This standard, ISO 15693, contains three sections: physical characteristics, air interface and

initialization, and anti-collision and transmission protocol. Accepted in 2000, it adopts a 13.56 MHz frequency spectrum, and has found some implementation among passive RFID systems. [7]

Frequency Bands

In addition to political restrictions on frequency use, there are technical considerations that must be evaluated prior to selecting an RF band for use with RFID. Each band has certain advantages as well as disadvantages. Range and penetration are the greatest variables among different frequencies. Within this context, the general rule is that the higher the frequency the higher the unobstructed range but the less likely the signal is to penetrate objects. In addition, interference from other sources within the same frequency range, reader/tag orientation, power levels, and data rate are directly affected by the frequency used. Table 3 summarizes the general characteristics of low and high frequencies.

	Low Frequency < 500 kHz	High Frequency > 1 MHz
Range	Short to Medium	Medium to Long
Date Rate	Medium	Fast
Orientation	Not Sensitive	Sensitive
Penetration	More	Less
Power Reqd	Low	High
Price	Inexpensive	Expensive
Noise Sensitivity	Yes	No

Source: The Cutting Edge of RFID

Table 3 – Summary of Frequency Implications to RFIDs

RFIDs presently can be found in four different frequency ranges: 125-134 kHz, 13.56 MHz, 2.45 GHz, and 5.8 GHz. These are now discussed in turn.

125-134 kHz

These fall within the low frequency range and are primarily used for passive tags. Communications with these tags rely upon “inductive (essentially magnetic) coupling” [10]. This results in these tags being primarily short-range (<4 meters) due to power levels, the need to sense the inductive signature, and the fact that the return is diffuse omni-directionally from the RFID tag. While the tags themselves cost approximately $1.00 each, this frequency suffers from a “smeared” electromagnetic field and as such require expensive readers with a “very sophisticated anti-collision signal processing algorithm” [10]. Finally, this spectrum does not provide for very fast transfer rates. This results in a smaller amount of data being able to be stored and processed if the objects are moving. On the positive side, these frequencies are unregulated, thus allowing for global use [3].

13.56 MHz

This frequency band falls within the high frequency component of RF and is already used for smart cards and labels. This band also relies (primarily) upon inductive coupling and requires expensive readers (normally of the enclosed type) to overcome interference. A benefit for this frequency range is that the tags used are generally less expensive, costing approximately $0.70 each [10].

2.45 GHz

This range is also considered high frequency, but is presently used for toll collection within the United States [5]. Its method of communication is propagation coupling, which means that the information transmitted is carried on the RF signal itself. This allows for greater data rates, and is normally performed through the use of directional antennas for open-air interrogation [10]. This band is also common for other uses, such as microwaves, telephones, and

WiFi computer networking. As such, inexpensive hardware (especially antennas) is widely available.

5.8 GHz

This frequency is not available for RFID use within the United States and is thus not covered in this paper. However, it is worth noting that this band is used throughout the European Union and is their toll road standard [5].

RFID Technical Impediments

There are a number of technical problems associated with RFID besides those of politics (e.g. standardization) and economics. Two of the greatest challenges lie in antenna design given such a small footprint and collision among multiple readers attempting to interrogate thousands of IDs.

Antenna Shortcomings [11]

Ultimately the range that can be achieved with an RFID system is determined by the power available at the reader, the power available within the tag to respond, and the environmental conditions or structures in the vicinity [12]. The antennas immensely impact the power available both at the reader and the RFID tag. Exacerbating the situation is the fact RFID frequencies are primarily in the microwave range. This portion of the electromagnetic spectrum is sensitive to antenna design, form, and electrical properties. Figure 6 illustrates three RFID antenna designs of increasing geometric complexity. The overall purpose of any antenna, and especially for those dealing with such low power levels as RFIDs, is to

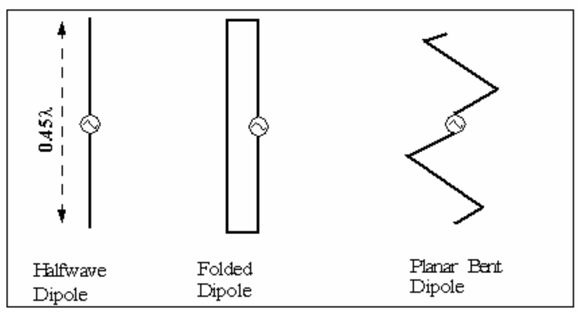

Figure 6 - Antenna Designs [11]

maximize “the transfer of power into and out of the device.” For such an application, the following criteria must be met:

- Small
- Hemispheric Coverage Pattern
- Maximum Signal Throughput (i.e. Minimal Attenuation)
- Polarized such that Orientation to Reader is Insignificant
- Robust
- Inexpensive

As can be imagined, such a design is difficult to realize. When seeking to meet these goals, the following four characteristics must be decided upon:

- Antenna Type
- Impedance
- RF Performance in Isolation
- RF Performance amid Physical Obstructions

Foster and Burberry, two prominent British electrical engineers, perform an outstanding analysis of the various antenna types and their acceptability for use in RFID applications in their paper “Antenna Problems in RFID Systems” [11]. The paper concludes in determining that directional antennas are best when scanning a particular area, while omnidirectional can serve a wider application but be prone to greater levels of cross-talk and interference.

Reader Collisions

The reader collision problem is defined as the “problem of allocating frequencies over time to Radio Frequency IDentification (RFID) tag readers such that their interference with one another is minimized” [13]. Such interference comes in two main varieties: (1) reader-to-reader and (2) tag interference. In the former, interference occurs on one frequency due to two or more readers simultaneously attempting to communicate at that frequency. In the latter case, two or more readers are trying to interrogate a particular tag at the same time.

Reader-to-reader collisions are more common with passive tags as they require greater power to be injected into the air per unit tag. Passive tags are generally “dumb” devices in that

they are unable to perform any operations on their own, such as discriminating among readers and determining who to respond to. Thus their "reliance upon energy harvesting limits both the communication range and functionality" of these tags [13].

Tag interference is more common among active tags in that they have a greater range and are more likely to interact with multiple readers at a given instant in time. When this problem exists in isolation, it is said to be a "resource constrained scheduling problem" and solved using optimization methods.

Means do exist to solve or at least mitigate reader collisions. One such solution is the judicious allocation of frequency to readers to provide maximum separation among adjacent readers while also minimizing the duplicative assignment of any specific frequency. Another solution to this problem is the implementation of schemes, such as Time Division Multiple Access (TDMA) which "interleaves communication times on the same frequency" [13]. Overall, experts generally believe that reader collision problems faced within the RFID field are "simpler" than the frequency assignment problems faced by cellular telephone companies. If this is in fact the case, then finding solutions as reader collision situations arise should be more than feasible.

Security *and* Efficiency

One of the critical components to any increase in security is the balancing of enhancing security and the financial bottom line. Studies have demonstrated that while there does exist immediate short-term costs to adding technology to secure goods, the long-term forecasts identify a sum financial gain based not only on maintaining trade in the event of a catastrophic event, but improved gain in business practice efficiencies. These gains come on both a macro and micro level.

Comments on Security

There are quite a few built-in safeguards that protect the integrity of RFIDs, especially of the active variety. Secure RFIDs rely upon encryption to authenticate the tag itself (by signing with the tag's private key) as well as integrity (by using the server's public key to encrypt the data message). Additionally, an interruption in service automatically triggers an alarm. This encryption also protects against outsiders spoofing the RFID as the true public key of the RFID would not decrypt the message of the spoofing RFID. Finally, sensors continue to evolve and are providing more detailed, sophisticated, and comprehensive pictures of the cargo in transit.

Macro Level (Primarily Active) [14]

The big-picture gains from RFIDs come from the two significant improvements within such a system: dramatic increase in both the detail of information and the degree of automation. The unique codes allow for boxes, pallets, and containers to be rapidly tracked while in shipment. The greatest gains come in the area of security. RFIDs allow for the tracking of shipments in real time in order to ensure that they are following the correct route. The augmentation of sensors expands the ability to monitor the movement of goods. This results in greater levels of control of the supply chain and increased amounts of accurate information. Ultimately all of this results in greater knowledge about the contents, condition, and continuity of what is being tracked, bringing about safer ports and greater profits.

Micro Level (Primarily Passive)

Small-scale gains in converting to RFID modes of operation are best seen in contrast to the use of barcodes. RFID technology allows for much greater throughput, which has direct monetary benefits. Additionally, the higher level of detail results in smarter inventory management. This provides a means of preventing "shrinkage" caused by "employee and

customer theft, vendor fraud, and administrative error," which accounts for a loss of nearly two percent of total sales [14]. Furthermore, a study by Gap clothing has found that having all the right sizes in the right place results in greater profits [15]. Thirdly, there is direct labor cost savings in the use of RFID tags. No time is needed to handle goods and scan them, while considerable labor costs are involved in a barcode system. It is estimated that RFID can decrease 25% of labor time used in inventory and sale transactions [15]. Thus the benefits of RFID at the micro-level can be summarized "in terms of labor savings, anti-diversion track-and-trace ability, and supply chain visibility" [15].

Beyond these efficiency savings, there are a number of external factors outlined in "Web-Based RFID: Hype or Glimpse of the Future?" that will serve as a catalyst in the adoption of RFID among retailers. The first deals directly with container security: the Customs and Border Patrol's Container Security Initiative. This push to digitize the trade documentation coupled with the 24-hour rule is placing increasing pressure to provide accurate manifests that are acquired in the most non-labor intensive method possible. RFIDs meet these needs. Secondly, on January 1, 2005, an additional digit will be added to barcodes, requiring the barcode infrastructure to upgrade. It is quite plausible that between now and then businesses will choose to either replace their barcode systems with RFID ones or install dual-functionality consoles. The third factor creating an environment conducive to RFID adoption at the unit level is the recently announced Electronic Supply Chain Manifest (ESCM) that will place the same documentation requirements on domestic trade as that of international. Its implementation is set for the 2005-2006 time frame [15]. The final factor is that of Wal-Mart's RFID Strategy. Wal-Mart is requiring that its top 100 suppliers must begin using RFID chips at least at the pallet level by January 2005. It is estimated

that if the “top 100 suppliers to the top 30 retailers” started using RFID, almost 80% of all consumer goods would be tagged!

There is some resistance to this among consumers, especially in the area of competitive concerns. In addition, there remains non-uniformity with regards to frequency and RFID information storage and retrieval. This lack of standardization is highlighted in the DOD’s use of ISO standards, of which none exists for RFID formats due to the number of standards presently available and lack of anyone capturing extensive market share [15].

Present RFID Applications

RFIDs with their low-power, short-range communications capabilities have already found use in a wide array of applications. In many cases their use is awkward and bulky, a situation that is surely to change with the advent of smaller and more convenient forms of RFIDs. In spite of this, RFID technology has found its way into everyday use. Many automobile manufacturers (such as Ford and Honda) now use RFID transponders in keys to validate the key used in the transmission. Should someone use a key that is properly cut but lacking the RFID, the car becomes demobilized, such as by cutting off the fuel [4]. This technology can also be used to limit the engine RPMs such as on a valet key or the radio volume on a teenager’s key. In some hospitals, babies are tagged with RFIDs as well as employees and parents to ensure the child is properly tracked and not taken to the wrong place by the wrong person. Some cities have

Access Control	embedded in personal ID cards
Baggage ID	embedded in paper luggage tags
Automotive Systems	keyless entry and immobilization systems
Document Tracking	Affixed to Documents
Express-Parcel Tracking	Truck Entry and Package Tracking
Library Book Control	Tags in Books
Livestock Tracking	Injected into Animals
Logistics and Supply Chain	Container and Product Tracking
Wireless Commerce	Mobil Speedpass and Car Tolls

Source: Pervasive Computing Goes the Last 100 Feet

Table 4 - Current RFID Uses

implemented RFIDs on police cars and other emergency vehicles to synchronize the stop lights to allow safe and expedited passage during an emergency [4]. A final example to expound is the use of RFIDs in automobile toll plazas. Georgia Interstate 400 uses such technology to provide for quicker toll collection and transit times. A summary of current uses is listed in Table 4.

Future in RFID

Smart Labels [5]

Smart Labels seek to replace barcodes in the tracking of consumer items from ketchup to Nikes. They are an inexpensive solution for those who are looking to track millions of items. Their features include:

- Cost tens of Cents
- Produced in High Volume
- Thin and Flexible
- Read and Write Capability
- Simultaneous Read
- Easy to Integrate with Barcode Infrastructure

Potential applications include:

- Airline Baggage Tracking
- Express Parcel ID and Tracking
- Product ID Tracking from "Womb to Tomb"
- Brand Authentication
- Document Tracking
- Library Material Handling

Ultra Small Chips [16]

A special subset of smart labels is that of microchips. Beyond simply being affixed to a product, as is the case with the labels, microchips allow for complete integration. Prototype microchips of today use advanced semiconductor technology to incorporate complete RFID tags in 0.06 mm thick and 0.4 mm sided square (see figure). These

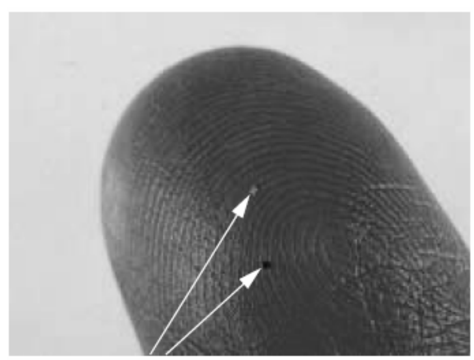

Figure 7 - Two Prototype Microchips. Both .4 x .4 mm

prototype µ-chips operate in the 2.45 GHz band, contain 128 bits of unrewritable storage, and present an additional host of potential applications including:

- Forgery Prevention (ex. Art, Currency)
- Imbedded RFID (ex. Artificial Limbs, Clothing)
- Unobstructed Document Tracking (imbedded in paper)
- Personal Identification and Finances (imbedded in people)

Privacy Concerns

Needless to say, “total visibility” of objects from production to shipment to point of sale can also mean “total visibility” after the sale. This has raised the concern of many parties, as all could potentially be affected by the pervasive deployment of RFID tags. Both private citizens and companies have a compelling interest in this issue. Not only could covert, pervasive readers track people’s buying habits, dress habits, and basic living habits, but entire store inventories could be captured by competing interests or industry shipments tracked. This problem is only compounded by efforts to place all of this information online for real-time data harvesting [15].

Computer experts, however, believe that it is possible to protect the privacy of citizens, but only if they demand so [7]. An example of this can be found when the clothing chain Benetton announced plans to insert RFIDs in all their clothing. The public outcry was overwhelming and they were forced to suspend their plan [7]. The technology to encrypt data, only respond to interrogations by coded scans, and disable RFIDs after purchase exist. However with the technology immature and constantly under development, the constant pressure must be applied to ensure privacy is balanced with needed security.

Future Deployment of RFID for Container Security

Presently there are a series of programs being sponsored by the Department of Homeland Security and the Department of Transportation to prototype commercially available technologies for near-immediate deployment. The Container Security Initiative is the largest example of this. One of the greatest problems within the Information Age is managing the vast quantities of electronic data and using it, coupled with human intelligence, to discern usable information. The port of Charleston, SC has been selected to stand-up an integrated command center, known as Seahawk, which seeks to accomplish this.

Figure 8 - Port of Charleston

Project Seahawk [17]

Project Seahawk is a $9 Million effort to integrate the efforts of all law enforcement agencies in the Charleston area with an interest in maritime and/or security in order to provide an informed managerial structure and coordinated security effort. As the fourth largest port (by Twenty-Foot Equivalent Units), Charleston is well positioned to be the location for Project Seahawk. The main components of the project are:

- Creation of unified federal, state, local law enforcement **task force**
- Formation of **data sharing system** from participating agencies data bases for vessel, crew, and cargo tracking, targeting, inspecting, and investigations
- Establishment of fusion **operations center** for marine and intermodal transportation domain awareness
- Institution of unified **communications system**

While RFID's are not specifically part of this project, technology does play a critical role in this project's success and ultimately the data systems being developed for this unified operations center could provide the infrastructure for intelligently managing RFID data in the future.

Conclusion

Technology truly is a double-edged sword. There are many things humans can do today that simply weren't even imaginable fifty, twenty, or even ten years ago; this is not always a good thing. Fortunately the human mind is without limits, and as new threats and amoral individuals surface, so too do new defenses. RFID shows much promise in revolutionizing the way business is conducted. More so, while not the panacea of container trade security, it has been demonstrated by GTRI and others to be a valuable component of increasing the amount of valuable information available and strengthening the security of our ports, our economy, and our lives. One only hopes it is implemented before it is too late.

Disclaimer:

The views expressed herein are those solely of the author and are not to be construed as official or reflecting the views of the Commandant, the United States Coast Guard, or any agency of the United States Government.

References

[1] Binnendijk, Hans et al. "The Virtual Border: Countering Seaborne Container Terrorism." Defense Horizons (August 2002): 1-12.

[2] "Container Security Report." CISAC Report. Stanford Study Group (January 2003).

[3] Stromgren, Chel. "Cargo Handling Cooperative Program." SAIC (23 August 2002).

[4] Ollivier, M. M. "RFID – A Practical Solution for Problems You Didn't Even Know You Had!" Texas Instruments Ltd, UK.

[5] d'Hont, Susy. "The Cutting Edge of RFID Technology and Applications for Manufacturing and Distribution." Texas Instruments TIRIS.

[6] "Active and Passive RFID: Two Distinct, but Complimentary, Technologies for Real-Time Supply Chain Visibility." Savi Technology (January 2002).

[7] Stanford, Vince. "Pervasive Computing Goes the Last Hundred Feet with RFID Systems." IEEE Pervasive Computing (April-June 2003): 9-14.

[8] Buckner, Mark, et al. "MICLOG RFID Tag Program Enables Total Asset Visibility." IEEE Explore (2002): 1422-1426.

[9] Mercuri, Rebecca. "Standards Insecurity." Communications of the ACM (December 2003): 21-25.

[10] Cerino, Anthony and William Walsh. "Research and Application of RFID Technology to Enhance Aviation Security." IEEE Explore (2000): 127-135.

[11] Foster, P. and R. Burberry. "Antenna Problems in RFID Systems." IEE (1999).

[12] Ni, Lionel et al. "LANDMARC: Indoor Location Sensing Using Active RFID." Proceedings of the First International Conference on Pervasive Computing and Communications (2003).

[13] Engels, Daniel and Sanjay Sarma. "The Reader Collision Problem." IEEE SMC (2002).

[14] Sahin, Evren et al. "Performance Evaluation of a Traceability System." IEEE SMC (2002).

[15] Akinson, William. "Web-Based RFID: Hype or Glimpse of the Future?" Apparel (February 2003).

[16] Takaragi, Kazuo et al. "An Ultra Small Individual Recognition Security Chip." IEEE Micro (November – December 2001): 43-49.

[17] Interview with CDR Beeson on 24 March 2004.

[18] Raza, Nadeem et al. “Applications of RFID Technology.” IEE (1999).

[19] Interview with Dr. Giselle Bennet on 01 April 2004.

Bibliography

Johnson, Andrew. “Non-Intrusive Cargo Inspection.” IEEExplore (1995): 61-68.

Kwak, Sung-Woo. “Solid-State Detector Design for Mobile Cargo Container Inspection System Using Medium Energy X-Ray.” IEEExplore (2003): 475-479.

Brown, David. “Human Occupancy Detection.” IEEExplore (1995): 166-174.

“Expansion of Key Customs Programs will Require Greater Attention to Critical Success Factors.” GAO (July 2003).

Brew, Nigel. “Ripples from 9/11: the US Container Security Initiative and its Implications for Australia.” Department of the Parliamentary Library (13 May 2003).

“Operation Safe Commerce” Web Page. <www.tsa.gov/public/display?content=090005198006aale> (24 March 2004)

“Fact Sheet: U.S. Customs Service’s Container Security Initiative.” 22 February 2002 <http://usinfo.state.gov/topical/pol/terror 02022505> (05 April 2004).

“C-TPAT Home Page” <www.chb.gov/xp/cgov/import lines> Whem things Frequently asked questions are kept to maintain confidentiality.

Schoemann, Lee and Sorokowski, Donald. “Authenticated Tracking and MonitoringSystems (ATMS). IEEE (231-240).

“Automated Targeting System.” <www.customs.ustreas.gov> (05 April 2004)

Yasuura, Hiroto et al. “Towards the Digitally Names World – Challenges for New Social Infrastructures based on information secretly.” IEEE Computer Society (2003).